WHAT IS CLAIMED IS:

1. A data processing system, comprising:

at least one main processor connected to a system bus;

a system memory connected to the system bus and accessible to each of the main processors;

a tamper mechanism configured to change state responsive to insertion of the system into a slot in a rack enclosure; and

a local service processor, connected to the tamper mechanism and configured to update an insertion log responsive to detecting a changed state of the tamper mechanism, wherein the insertion log provides a history of at least some rack insertions to which the system has been subjected.

2. The system of claim 1, further comprising a non-volatile storage element accessible exclusively to the local service processor and containing the insertion log.

3. The system of claim 2, wherein the insertion log includes an insertion counter, and wherein the local service processor is configured to increment the insertion counter upon each insertion.

4. The system of claim 3, wherein the local service processor is configured to issue an alert responsive to the insertion counter exceeding a predetermined value.

5. The system of claim 1, further comprising a battery backed real-time clock connected to the local service processor, wherein the local service processor is configured to include real-time information corresponding to each insertion event in the insertion log.

6. The system of claim 1, wherein each entry in the insertion log includes the identity of the rack enclosure and the geographical address of the slot of the corresponding insertion event.

7. The system of claim 1, wherein the local service processor is configured to detect the tamper mechanism state and update the insertion responsive to a power event such that the insertion log update is independent of configuring the data processing system with a boot image.

8. A data processing network, comprising:

a plurality of server blades connected to a common network, each blade comprising at least one main processor connected to a system bus, a system memory connected to the system bus and accessible to each of the main processors, a tamper mechanism configured to change state responsive to insertion of the system into a slot in a rack enclosure; and a local service processor, connected to the tamper mechanism and configured to update an insertion log responsive to detecting a changed state of the tamper mechanism, wherein the insertion log provides a history of at least some rack insertions to which the system has been subjected.

9. The network of claim 8, further comprising a non-volatile storage element accessible exclusively to the local service processor and containing the insertion log.

10. The network of claim 9, wherein the insertion log includes an insertion counter, and wherein the local service processor is configured to increment the insertion counter upon each insertion.

11. The network of claim 10, wherein the local service processor is configured to issue an alert responsive to the insertion counter exceeding a predetermined value.

12. The network of claim 8, further comprising a battery backed real-time clock connected to the local service processor, wherein the local service processor is configured to include real-time information corresponding to each insertion event in the insertion log.

13. The network of claim 8, wherein each entry in the insertion log includes the identity of the rack enclosure and the geographical address of the slot of the corresponding insertion event.

14. The network of claim 8, wherein the local service processor is configured to detect the tamper mechanism state and update the insertion responsive to a power event such that the insertion log update is independent of configuring the data processing system with a boot image.

15. A computer program product comprising a set of computer executable instructions for logging server blade insertions in a data processing network, the instructions being stored on a computer readable medium, comprising:

computer code means for determining the state of a tamper latch of the server blade; and

computer code means, responsive to detecting a tamper latch state change, for updating an insertion log wherein the insertion log is local to the server blade and provides a history of at least some rack insertions to which the system has been subjected.

16. The computer program product of claim 15, wherein the insertion log comprises at least a portion of a non-volatile storage element accessible exclusively to the local service processor.

17. The computer program product of claim 16, wherein the insertion log includes an insertion counter, and wherein the computer program product is configured to increment the insertion counter upon each insertion.

18. The computer program product of claim 17, wherein the code means is configured to issue an alert responsive to the insertion counter exceeding a predetermined value.

19. The computer program product of claim 15, wherein each entry in the insertion log includes the identity of the rack enclosure and the geographical address of the slot of the corresponding insertion event.

20. The computer program product of claim 15, wherein the local service processor is configured to detect the tamper mechanism state and update the insertion responsive to a power event such that the insertion log update is independent of configuring the data processing system with a boot image.

5